REMARKS

Applicant respectfully requests reconsideration of the application.

Claim 2 is rejected under 35 U.S.C. Section 112 as being indefinite. The Office contends that it is not clear whether the forensic watermark identifies the receiver or the content signal. Applicant contends that the claim clearly indicates that the forensic watermark identifies the receiver. However, this rejection is moot in view of the amendment that recasts the claim language.

Claims 1-3, 5-12 and 14-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,373,960 to Conover in view of 6,898,706 to Venkatesan et al. ("Venkatesan").

Applicant submits that Venkatesan does not teach the elements of claim 1 that are acknowledged to be missing from Conover. In addition, the existence of a motivation or suggestion to combine these references is lacking because the watermarks are used for significantly different reasons in these references, which greatly impacts how the watermarks are embedded as discussed below.

Claim 1 recites embedding a forensic digital watermark to robustly associate a content signal with the receiver, wherein the embedding applies a different orientation for different instance of embedding the forensic digital watermark. The Examiner correctly acknowledges that Conover does not teach these aspects of claim 1, yet contends that Venketesan's use of keys corresponds to these elements of claim 1.

Venketesan uses a digital watermark in an electronic object not as a robust forensic digital watermark, but instead, as part of an access control mechanism to control access to the electronic object. Venketesan clearly states that all n watermark keys are identical across all objects to be protected. See column 6, lines 2-4. Thus, regardless of the receiver that receives this electronic object, the n watermark keys are identical. This refutes the Office's position that Venketesan's use of keys somehow applies a different orientation for different instances of embedding a forensic digital watermark.

Further, in Venketesan, the watermark is embedded n times in an object before the object is distributed. When the object is received at a client, one of keys is used to determine whether the client will have access to the object. The client does not embed a forensic digital watermark as claimed.

In addition, the orientation aspect of claim 1 is further defined as follows: "the orientation varies for different receivers to reduce interference between overlapping forensic digital watermarks embedded in the content signal by different receivers." As noted above, Venketesan does not teach varying the orientation for different receivers. In addition, Venketesan provides no teaching regarding selecting an orientation to reduce interference between overlapping forensic digital watermarks embedded in the content signal by different receivers. Venketesan does not even encounter this problem of interference because it embeds the n watermarks prior to distribution of the object, and therefore, there is no anticipated problem of over-embedding additional watermarks at the receiver. If a receiver did embed another watermark overlapping one or more of these n watermarks, it would likely defeat Venketesan's access control scheme because it would either change the value of that watermark or render it unreadable. This would lead to improperly blocking access to the object or improperly allowing access to an object. For example, Venketesan blocks access where the watermark data does not match expected data, possibly leading to improper blocking of access. See column 6, lines 63-65. As another example, if the watermarks interfered making the watermark unreadable (and thus appearing to be un-watermarked), then the receiver is allowed to freely access the object, which also undermines the access control system. See column 6, lines 47-49. In short, Venketesan deals with a different use of a watermark (to provide access control rather than robustly associate content with a receiver) and does not provide robustness to interference of overlapping forensic watermarks as claimed.

Independent claims 10 and 19, though having different elements and scope, are patentable over Conover and Venketesan for similar rationale as claim 1.

Dependent claims 2-3, 5-9, 11-12, 14-18 and 20 recite additional novel combinations that further distinguish the cited art. For the sake of brevity, these distinctions are not belabored here.

Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Conover in view of Venketesan and further in view of U.S. Patent Publication 20020027994 by Katayama et al. ("Katayama"). Katayama does not teach the elements missing from Conover and Venketesan, and therefore, the combination does not teach all of the elements of claims 4 and 13.

Claims 1-3, 5-8, 10-12 and 14-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,801,999 to Venkatesan et al. ("Venkatesan 999") in view of Fenghhi et al. "Digital Certificates Applied Internet Security, 1999, ISBN: 0201309807 ("Fenghhi"). The above comments and the arguments provided previously refute the Office's position with respect to Venketesan 999 and Fenghhi.

The Office contends that the watermark authority in Venketesan 999 corresponds to a receiver in the claims. However, the claims refer to different receivers and the orientation is selected so that the orientation varies for different receivers. In Venketesan, the watermark authority applies n watermarks to an object, and it is not watermarked again. Further, these watermarks are used for access control, not to identify the receiver or robustly associate an object with the receiver. Thus, Venketesan does not even remotely encounter nor address the problem that the claims solve, namely, interference among watermarks applied by different receivers. Venketesan does not suggest that watermarks might be applied by different receivers, and in fact, it would undermine Venketesan's access control scheme to embed overlapping watermarks in different receivers as described above.

The Office suggests that Fenghhi is combinable with Venketesan because it purportedly teaches a plurality of authorities. The Office's rationale for combining Fenghhi with Venketesan is flawed. It states that one would be motivated to use the alleged authorities in Fenghhi to make Fenghhi scalable. This rationale has no bearing on the teachings of Venketesan 999 because it does not explain why one of ordinary skill in the art would be motivated to redress the acknowledged deficiencies of Venketesan 999 using the teachings of Fenghhi.

Perhaps more importantly, Fenghhi does not address the significant deficiencies in Venketesan 999 with regard to addressing the issue of reducing interference among forensic watermarks embedded by different receivers. Moreover, there is no basis in these references for combining Venketesan's watermark technique for access control with Fenghhi's teachings about using certificates to establish trust in particular data because these teachings are both unrelated to each other and the invention. Further, even if one combined Venketesan's teachings with Fenghii's, one would not modify Venketesan's system to embed keys in the object with different watermarking authorities, because, as explained above, this would likely undermine Venketesan's access control scheme.

Claims 4 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venketesan in view of Fenghhi and further in view of Katayama. Katayama does not teach the elements missing from Venketesan and Fenghhi, and therefore, the combination does not teach all of the elements of claims 4 and 13.

Claims 9 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan in view of Fenghhi and further in view of U.S. Patent Publication 20010009581 by Hashimoto ("Hashimoto"). Hashimoto does not teach the missing elements of the primary references, and therefore, the combination does not teach all of the elements of claims 9 and 18.

In view of the above, the claims are allowable over the applied prior art.

Respectfully submitted,

Date: November 27, 2006

Customer Number 23735

Telephone: 503-469-4800
FAX: 503-469-4777

DIGIMARC CORPORATION

By ______________________
Joel R. Meyer
Registration No. 37,677